Exercises for Group, polynomial, and Hamming codes

6^{th} January, 2006

1. Given a generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Find the parity check matrix, then all code words generated by the generator matrix above, and then find the dual code to that code.

2. Check whether 974-93880-3-8, 974-93880-4-6 and 0-1392-4101-4 are ISBN's.

3. Find the missing digits in the following ISBN's, 974-912¤7-4-3 and 974-9¤3¤1-8-4.

4. Construct tables of multiplicative inverses for $GF(5)$ and $GF(11)$.

5. Find a primitive element for each of $GF(5)$ and $GF(13)$.

6. Find the parity check matrix of the matrix code given by the generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

7. The parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

defines a code $E : \mathbf{F}_2^3 \to \mathbf{F}_2^6$. Find all the code words. Does the code thus resulted correct all single errors?

8. The *exponent* of a polynomial $g(x) \in \mathbf{F}_2[x]$ is the least positive integer e such that $g(x)|x^e - 1$. Find the exponent of the polynomials $a(x)$, $b(x)$ and $c(x)$ in $\mathbf{B}[x]$, when $a(x) = 1 + x + x^2$, $b(x) = x + x^3$ and $c(x) = 1 + x^2 + x^4$.

9. Given an encoding polynomial $g(x) = 1 + x^2 + x^3$. Find the generator matrix G of the $(4, 7)$ polynomial code. Then find the parity check matrix H of the code thus generated.

10. Find the binary equivalence of the decimal numbers 543, 25, 87 and 166.

11. Find the decimal representation of the binary numbers 11001110, 10100101, 10001100 and 10111.

12. Find all the code words of the binary $(3, 5)$ Hamming code.

13. Find a parity check matrix of the binary $(9, 13)$ Hamming code.

14. Write a parity check matrix for the 7-ary $(8, 6)$-Hamming code, then use it to decode the received vectors 54326010 and 11063452.

Reference

Raymond Hill. *A first course in coding theory.* Clarendon, 1986

L R Vermani. *Elements of algebraic codng theory.* Chapman & Hall, 1996